IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

Tara Bennett, David Garcia, and Edward Polhill, individually and on behalf of all others similarly situated, Plaintiffs, vs. T-Mobile USA, Inc., Defendant.	CIVIL FILE ACTION NO. 2:22-cv-1805 **CLASS ACTION** JURY TRIAL DEMANDED

COMPLAINT

Plaintiffs, on behalf of themselves and all others similarly situated, file this Class Action Complaint ("Complaint") against T-Mobile USA, Inc. ("T-Mobile") for declaratory judgement, injunctive relief, damages, and other equitable relief. Based upon personal knowledge of the facts pertaining to Plaintiffs and the investigation of counsel, Plaintiffs allege as follows:

INTRODUCTION

1. This is a class action brought by Plaintiffs on behalf of all T-Mobile customers that have been the victim of SIM swap fraud. This action arises because of T-Mobile's systemic and repeated failures to protect and safeguard its

customers' sensitive personal and financial information against common, widely reported, and foreseeable attempts to illegally obtain such information.

2. As a result of T-Mobile's misconduct as alleged herein, including its gross negligence in protecting customer information, its negligent hiring and supervision of T-Mobile employees who were responsible for safeguarding that information, and its violations of federal and state laws designed to protect wireless service consumers, Plaintiffs have lost millions of dollars and T-Mobile customers continue to suffer repeated instances of identity theft.

3. T-Mobile is one of the three largest providers of wireless services in the United States. As a leading wireless service provider, T-Mobile is required by law to protect the personal and financial information of its customers. And T-Mobile regularly holds itself out to the general public as a secure and reliable custodian of customer data. For example, T-Mobile promises its customers that it uses a variety of administrative, technical, contractual, and physical security measures to protect customers' personal and financial information against illegal, fraudulent, or unauthorized activities; to investigate suspicious traffic, cybersecurity threats or vulnerabilities, complaints, and claims; and to authenticate credentials for account access and information and provide other security protections.

4. As T-Mobile is aware, various forms of account takeover fraud have been widely reported in the press, by government regulators, and in academic publications. They have also been the subject of numerous lawsuits across the country. Typically, the purpose of these schemes is to compromise customers' mobile identities, access confidential data, take over their financial accounts, and effectuate fraudulent transactions.

5. One of the most damaging and pervasive forms of account takeover fraud is known as a "SIM-swap", whereby a third-party (with the help of a wireless carrier, like T-Mobile) is allowed to transfer access to a customer's wireless phone number from the customer's registered "subscriber identity module" card (or "SIM card")[1] to a SIM card controlled by the third party.

6. Once the third party has control over the customer's phone number, the third party has access to customer's call and text message history and can seamlessly impersonate the customer when communicating with others. But, perhaps most importantly, the third party also has the ability to control the text-based two-factor authentication checks specifically designed to add a layer of protection to sensitive accounts, such as bank accounts, cryptocurrency accounts, and e-mail accounts.

[1] The term SIM card is used herein to refer to a traditional physical SIM card or an embedded SIM card hardwired inside the phone.

7. A "SIM-swap" is not an isolated criminal act by the third party, as it requires the wireless service provider to reassign the customer's phone number from the SIM card in the customer's phone to a SIM card controlled by the third party. Thus, SIM-swaps are ultimately effectuated by the wireless service provider itself.

8. Contrary to its representations and in violation of the law, T-Mobile abjectly failed to protect Plaintiffs' personal and financial information. T-Mobile failed to implement and/or practice policies and procedures to sufficiently protect Plaintiffs' sensitive information and it failed to adequately train and supervise its employees, who repeatedly provide unauthorized access to illegal actors. T-Mobile's actions and/or failure to act demonstrate reckless disregard for the rights of Plaintiffs and T-Mobile's obligations and duties under the law.

9. As a result of T-Mobile's breaches of security, Plaintiffs lost millions of dollars and have been subjected to repeated attacks on their accounts that deprived them of access to their cell phones and exposed their personal and financial information to thieves.

10. Accordingly, Plaintiffs seek damages and equitable relief on behalf of themselves and those similarly situated, as well as declaratory relief that (1) T-Mobile's onerous arbitration provisions, including any delegation clause purportedly determining the scope of the arbitrator's authority, are procedurally

and substantively unconscionable and unenforceable as against Plaintiffs; and (2) T-Mobile's class action waiver and jury trial waiver are unenforceable as a matter of law. Plaintiffs also seek actual damages, statutory damages, punitive damages, restitution, and all applicable interest thereon, along with attorneys' fees, costs, and expenses; as well as injunctive relief, including significant improvements to T-Mobile's security systems and protocols, future annual audits, T-Mobile-funded long-term credit monitoring services, and any other remedies the Court deems necessary and proper, up to and including the appointment of a corporate monitor.

PLAINTIFFS

11. Plaintiffs bring this action on behalf of themselves, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

12. Plaintiffs are current and former customers of T-Mobile.

13. Plaintiff Tara Bennett ("Bennett") is a citizen and resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

14. Plaintiff David Garcia ("Garcia") is a citizen and resident of the state of California and has been a California resident at all times relevant to this Complaint.

15. Plaintiff Edward Polhill ("Polhill") is a citizen and resident of the state of Michigan and has been a Michigan resident at all times relevant to this Complaint.

DEFENDANT

16. Defendant T-Mobile is the operating entity of T-Mobile International AG & Co. in the United States. T-Mobile is a Delaware corporation with a principal place of business located in Bellevue, Washington.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The aggregate amount-in-controversy, exclusive of costs and interests, exceeds the sum of $5,000,000.00 and this is a class action in which at least one member of the proposed class is a citizen of a State different than Defendant.

18. Pursuant to 28 U.S.C. § 1331, this Court also has federal question subject matter jurisdiction because this Complaint asserts claims under the Federal Communications Act ("FCA") and the Computer Fraud and Abuse Act ("CFAA").

19. The Court has supplemental jurisdiction over Plaintiffs' state-law claims pursuant to 28 U.S.C. § 1367.

20. This Court has personal jurisdiction over T-Mobile because T-Mobile is a resident of the State of Washington.

21. Venue is proper in this District, pursuant to 28 U.S.C. § 1391, because T-Mobile maintains its principal place of business in Bellevue, Washington.

FACTUAL ALLEGATIONS

Background on T-Mobile

22. T-Mobile markets and sells wireless cellular phone service through standardized wireless service plans via various retail locations, online sales, and over the telephone.

23. T-Mobile maintains accounts for its wireless customers, enabling them to access information about the services they purchase from T-Mobile.

24. As one of the nation's largest wireless carriers, T-Mobile's operations must comply with various federal and state statutes, including (but not limited to) the Federal Communications Act ("FCA") 47 U.S.C. §222.

25. The FCA obligates T-Mobile to protect the "confidential proprietary information of [its] customers" and "customer proprietary network information" (commonly referred to as "CPI" and "CPNI", respectively). See 47 U.S.C. §222(a), (c).

26. The Federal Communications Commission ("FCC") has promulgated rules to implement Section 222 of the FCA "to ensure that telecommunications

carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." 1998 CPNI Order, 13 FCC Rcd. at 8195 ¶193; see also 47 C.F.R. §64.2001 et seq. ("CPNI Rules").

27. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. See 47 C.F.R. §64.2005.

28. The CPNI Rules also require carriers to implement safeguards to protect customers' CPNI. See 47 C.F.R. §64.2009(b), (d), and (e).

29. These safeguards include: (a) training personnel "as to when they are and are not authorized to use CPNI"; (b) establishing "a supervisory review process regarding carrier compliance with the rules"; and (c) filing annual compliance certificates with the FCC. *Id.*

30. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." See 47 C.F.R. §64.2010(a).

31. T-Mobile regularly holds itself out to the general public as a secure and reliable custodian of customer data, including customer's confidential financial and personal information.

32. T-Mobile maintains that it uses a variety of "administrative, technical, contractual, and physical safeguards" to protect customers' data "against security incidents, and illegal, fraudulent, or unauthorized activities; investigate suspicious traffic, cybersecurity threats or vulnerabilities, complaints, and claims; authenticate your credentials for account access and information and provide other security protections, as of August 9, 2021. *See* https://www.t-mobile.com/privacy-center/our-practices/privacy-policy.

33. As an example, T-Mobile explicitly states that "when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access."

34. Upon information and belief, T-Mobile's sales and marketing materials make similar representations regarding T-Mobile's alleged implementation of various safeguards to protect its customers' private information (as required by statutes). For example, T-Mobile's sales and marketing materials state: "We have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information."

35. Despite T-Mobile's obligations and representations, T-Mobile failed to provide reasonable and appropriate security to prevent unauthorized access to

customer accounts. Under T-Mobile's procedures, an unauthorized person, including T-Mobile's own agents and employees, acting without the customer's permission, can be authenticated and then can access and make changes to all the information to which the legitimate customer could access and make changes. T-Mobile also failed to disclose or disclosed misleading information to hide that its automated processes or human performances often fall short of its expressed and implied representations or promises, and such failures should have been foreseen by T-Mobile. Such failures, which lead to unauthorized access of customers' information, were entirely foreseeable by T-Mobile.

SIM Card Swaps

36. As T-Mobile is aware, various forms of account takeover fraud have been widely reported in the press, by government regulators (including the Federal Trade Commission ("FTC") and the FCC), academic publications, and multiple lawsuits across the country.

37. These illegal schemes involve criminals and fraudsters gaining access to or "hijacking" customer wireless accounts, which often include sensitive personal and financial information, to induce third parties to conduct transactions with individuals they believe to be legitimate or known to them.

38. Sometimes these schemes are perpetrated by employees of the wireless carriers, such as T-Mobile.

39. One of the most damaging and pervasive forms of account takeover fraud is known as a "SIM-Swap", whereby a third-party (with the help of a wireless carrier like T-Mobile) is allowed to transfer access to a customer's cellular phone number from the customer's registered "subscriber identity module" card (or "SIM card") – to a SIM card controlled by the third party.

40. A SIM Card has a complete record of a user's cell phone history, inclusive of text messages, calls, and any Apps which a user has downloaded.

41. A SIM swap is when a hacker convinces a carrier to switch a phone number over to a SIM card they own. Once a hacker has access to the phone number then they control the text-based two-factor authentication checks specifically designed to add a layer of protection to sensitive accounts such as bank accounts, social media accounts, and email accounts.

42. The wireless carrier, however, must effectuate the SIM card reassignment and, therefore, "SIM-swapping" is not an isolated criminal act, as it requires the wireless carrier's active involvement to swap the SIM containing information regarding its customer to an unauthorized person's phone.

43. Indeed, unlike a direct hack of data, whereby a company like T-Mobile plays a more passive role, SIM-swaps are ultimately effectuated by the wireless carrier itself. For instance, in this case, it is T-Mobile that approved and allowed the SIM card change (without Plaintiffs' authorization), as well as all of

the subsequent telecommunication activity that was used to access Plaintiffs' online accounts and cause the injuries suffered by Plaintiffs.

44. As such, by directly or indirectly exceeding the authorized access to customer accounts, wireless carriers such as T-Mobile may be liable under state and federal statutes, such as the FCA.

45. Once a third-party has access to the legitimate user's SIM card data, it can then seamlessly impersonate that legitimate wireless customer (e.g., in communicating with others or contacting various vendors), including by undermining the security customers have placed on their financial accounts, such as two-factor authentication through text messages.

46. In 2016, the FTC's Chief Technologist described these issues in a widely read post about her experience as a victim of an identity theft scheme and specifically called attention to the insidious "SIM-swapping" scheme in which thieves use a victim's hijacked phone number to gain access to financial accounts that use two-factor authentication through text messages. *See* "Your mobile phone account could be hijacked by an identity thief," Lorrie Cranor, FTC Chief Technologist (Jun 7, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief. T-Mobile was undoubtedly aware of this scheme and represented to its customers that they were protected against this type of identity theft.

47. As further described and acknowledged by the FTC's Chief Technologist Lorrie Craynor, "mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts…. Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions."

48. The prevalence of SIM-swap fraud and T-Mobile's knowledge of such fraud, including, but not limited to, that performed with the active participation of its own employees, demonstrate that what happened with Plaintiff's account was neither an isolated incident nor an unforeseeable event.

49. As a regulated wireless carrier, T-Mobile has a well-established duty – one which it freely acknowledges on its corporate website – to protect the security and privacy of CPI and CPNI from unauthorized access and T-Mobile is obligated to certify its compliance with this mandate to the FCC every year.[2]

50. The prevalence of SIM-swap fraud and T-Mobile's knowledge of such fraud, including, but not limited to, that performed with the active participation of its own employees, demonstrate that what happened with Plaintiff's account was neither an isolated incident nor an unforeseeable event.

[2] *See*, *e.g.*, https://www.t-mobile.com/privacy-center/education-and-resources/cpni.

51. As a regulated wireless carrier, T-Mobile has a well-established duty – one which it freely acknowledges on its corporate website – to protect the security and privacy of CPI and CPNI from unauthorized access and T-Mobile is obligated to certify its compliance with this mandate to the FCC every year.

52. The FCA expressly restricts carriers like T-Mobile from unauthorized disclosure of CPNI.

53. In light of the above, at the time of the events at issue in the present case, T- Mobile was keenly aware of its obligations, as well as multiple weaknesses in its internal processes and procedures to authenticate legitimate customers.

54. The failure of T-Mobile to have proper safeguards and security measures as recommended by the FCC resulted in damages to Plaintiffs, including but not limited to the loss of money and the compromising of personally identifiable information, in an amount to be determined at trial.

T-Mobile's Lack of Adequate Security

55. T-Mobile has been on notice for years that their security measures were not adequate. Despite this T-Mobile's procedures and practices, taken together, fail to provide reasonable and appropriate security to prevent unauthorized access to its customer wireless accounts, allowing unauthorized

persons to be authenticated and then granted access to sensitive customer wireless account data.

56. In particular, T-Mobile has failed to establish or implement reasonable policies, procedures, or regulations governing the creation and authentication of user credentials for authorized customers accessing T-Mobile accounts, creating unreasonable risk of unauthorized access. As such, at all times material hereto, T-Mobile has failed to ensure that only authorized persons have such access and that customer accounts are secure.

57. Among other things, T-Mobile:

a. failed to establish or enforce rules sufficient to ensure only authorized persons have access to T-Mobile customer accounts;

b. failed to establish appropriate rules, policies, and procedures for the supervision and control of agents and employees;

c. failed to establish or enforce rules, or provide adequate supervision or training, sufficient to ensure that all its employees or agents follow the same policies and procedures;

d. failed to adequately safeguard and protect its customer wireless accounts, including that of Plaintiffs, so unauthorized third parties were able to obtain access to their account;

e. permitted the sharing of and access to user credentials among T-Mobile's agents or employees without a pending request from the customer, thus reducing likely detection of, and accountability for, unauthorized accesses;

f. failed to suspend user credentials after a certain number of unsuccessful access attempts;

g. failed to adequately train and supervise its agents and employees, allowing its agents or employees, without authorization or approval, to unilaterally access and make changes to customer accounts as if the customer had so authorized;

h. allowed porting out of phone numbers without properly confirming that the request was coming from the legitimate customers;

i. failed to monitor its systems for the presence of unauthorized access in a manner that would enable T-Mobile to detect the intrusion, so that the breach of security and diversion of customer information was able to occur in the Plaintiffs' situation and continued until after their virtual currency account was compromised;

j. failed to implement simple, low-cost, and readily available defenses to identity thieves such as delaying transfers from accounts on which the password was recently changed or simply delaying transfers from accounts to allow for additional verifications from the customers;

k. failed to build adequate internal tools to help protect its customers against hackers and account takeovers, including protection from phone porting and wrongdoing by its own agents or employees acting on their own behalf or on behalf or at the request of a third party;

l. failed to implement processes and procedures for identifying red flag warnings of possible account takeovers and/or account compromise; and

m. failed to implement efficient and effective remediation in the event of account takeover and/or account compromise.

58. Due to the security practices and procedures described herein, T-Mobile established user credential structures that created an unreasonable risk of unauthorized access to customer accounts, including that of Plaintiffs.

59. On information and belief, T-Mobile has long been aware of the security risks presented by, inter alia, its weak user credential structures or

procedures. In addition, T- Mobile does not use readily available security measures to prevent or limit such attacks.

60. As a result of T-Mobile's faulty security practices, an attacker could easily gain access to a customer's account and then use it to gain access to the customer's sensitive information such as information used to access accounts at financial institutions, among other things.

61. T-Mobile's lack of adequate security enabled unauthorized third parties to access Plaintiffs' wireless accounts, which then enabled the unauthorized third parties to access Plaintiffs' other sensitive information, including virtual currency accounts, fiat bank accounts, private cloud data storage and computer accounts, and email services, where mobile phone numbers, text messages and phone call-back features are/were used as the first or second factor in two factor authentication (2FA) security schemes.

T-Mobile Gives Illegal Actors Unauthorized Access to Plaintiffs' Wireless Service and Phone Numbers

Plaintiff Bennett

62. T-Mobile provided Ms. Bennett wireless services, including a telephone number, for Ms. Bennett's mobile device.

63. Ms. Bennett stored personal information, including personally identifiable information, on her mobile device, used her mobile device to access

her financial accounts, and used her telephone number serviced by T-Mobile to secure accounts, including financial accounts, with other companies.

64. Upon information and belief, on or about February 17, 2022, a T-Mobile employee or agent gave an illegal actor access to Ms. Bennett's telephone number without Ms. Bennett's knowledge and/or authorization. Upon information and belief, T-Mobile swapped Ms. Bennett's mobile phone service from her device (which has a uniquely identifiable SIM card or embedded SIM) to the illegal actor's mobile device (which had a different SIM card).

65. As a result of T-Mobile's actions and omissions, Ms. Bennett has already suffered injury and remains at imminent risk of future harm, including monetary damages and the potential disclosure of personally identifiable information. Ms. Bennett lost secure and exclusive access to wireless service at her telephone number. After T-Mobile exposed Ms. Bennett's accounts with personal identifying information and assets, she lost over $14,000 worth of funds or assets. In addition, Ms. Bennett has spent time and effort monitoring her accounts for fraudulent activity and working to secure his accounts.

Plaintiff Garcia

66. T-Mobile provided Mr. Garcia wireless services, including a telephone number, for Mr. Garcia's mobile device.

67. Mr. Garcia stored personal information, including personally identifiable information, on his mobile device, used his mobile device to access his financial accounts, and used his telephone number serviced by T-Mobile to secure accounts, including financial accounts, with other companies.

68. Upon information and belief, on or about September 3, 2022, a T-Mobile employee or agent gave an illegal actor access to Mr. Garcia's telephone number without Mr. Garcia's knowledge and/or authorization. Upon information and belief, T-Mobile swapped Mr. Garcia's mobile phone service from his device (which has a uniquely identifiable SIM card or embedded SIM) to the illegal actor's mobile device (which had a different SIM card).

69. As a result of T-Mobile's actions and omissions, Mr. Garcia has already suffered injury and remains at imminent risk of future harm, including monetary damages and the potential disclosure of personally identifiable information. Mr. Garcia lost secure and exclusive access to wireless service at his telephone number. After T-Mobile exposed Mr. Garcia's accounts with personal identifying information and assets, he lost thousands of dollars' worth of funds or assets. In addition, Mr. Garcia has spent time and effort monitoring his accounts for fraudulent activity and working to secure his accounts.

Plaintiff Polhill

70. T-Mobile provided Mr. Polhill wireless services, including a telephone number, for Mr. Polhill's mobile device.

71. Mr. Polhill stored personal information, including personally identifiable information, on his mobile device, used his mobile device to access his financial accounts, and used his telephone number serviced by T-Mobile to secure accounts, including financial accounts, with other companies.

72. Upon information and belief, on or about December 1, 2021, a T-Mobile employee or agent gave an illegal actor access to Mr. Polhill's telephone number without Mr. Polhill's knowledge and/or authorization. Upon information and belief, T-Mobile swapped Mr. Polhill's mobile phone service from his device (which has a uniquely identifiable SIM card or embedded SIM) to the illegal actor's mobile device (which had a different SIM card).

73. As a result of T-Mobile's actions and omissions, Mr. Polhill has already suffered injury and remains at imminent risk of future harm, including monetary damages and the potential disclosure of personally identifiable information. Mr. Polhill lost secure and exclusive access to wireless service at his telephone number. After T-Mobile exposed Mr. Polhill's accounts with personal identifying information and assets, he lost over $5,000 worth of funds or assets. In addition, Mr. Polhill has spent time and effort monitoring his accounts for fraudulent activity and working to secure his accounts.

CLASS ACTION ALLEGATIONS

74. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following class (collectively, the "Class"):

> All current and former customers of T-Mobile for whom T-Mobile transferred control of the customer's phone number to a SIM card controlled by an unauthorized third party.

75. The following individuals and entities are excluded from the proposed Class:

> T-Mobile and T-Mobile's parents, subsidiaries, affiliates, officers and directors, and any entity in which T-Mobile has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

76. Plaintiffs reserve the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional sub-classes as warranted by further investigation.

77. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

78. Plaintiffs have no interests antagonistic to those of the Class.

79. **Numerosity**: T-Mobile has more than 100 million customers. The proposed Class is believed to be so numerous that joinder of all members is

impracticable. Upon information and belief, the total number of Class Members is in the thousands, if not tens of thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records.

80. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. All such claims arise out of the same systemic and repeated failures by T-Mobile to protect and safeguard its customers' sensitive personal and financial information against common, widely reported, and foreseeable attempts to illegally obtain such information. The same or similar documents are used by Defendant in its dealings with Plaintiffs and Class Members. Plaintiffs and all members of the Class were injured through T-Mobile's uniform misconduct, negligence, and breaches of duty.

81. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

82. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation.

It would be very difficult, if not impossible, for individual members of the Class to effectively redress T-Mobile's wrongdoing. Even if Class members could afford such individual litigation or even individual arbitration, the court system could not. Individualized litigation and/or arbitration presents a potential for wholly inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single forum.

83. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class. Those questions predominate over any questions that may affect individual members of the Class. Those common questions of law and fact include, without limitation:

a. Whether Defendant owed duties to Plaintiffs and the Class, the scope of those duties, and whether Defendant breached those duties;

b. Whether Defendant's conduct was unfair or unlawful;

c. Whether Defendant engaged in deceptive conduct;

d. Whether Defendant engaged in the wrongful conduct alleged herein;

e. Whether the Federal Communications Act ("FCA") and the Computer Fraud and Abuse Act ("CFAA") apply to Defendant;

f. Whether Defendant violated the FCA and CFAA;

g. Whether T-Mobile fails to employ adequate safety and security measures for its customers;

h. Whether T-Mobile has failed to establish or implement reasonable policies, procedures, or regulations governing the creation and authentication of user credentials for authorized customers accessing T-Mobile accounts, creating unreasonable risk of unauthorized access as set forth in para. 57 *supra*;

i. Whether the purported Terms and Conditions and its arbitration clause, including any delegation clause, are illegal, unconscionable, or otherwise unenforceable;

j. Whether Plaintiffs and the Class suffered injuries from Defendant's security breaches;

k. Whether declaratory and injunctive relief are appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class members and the public; and

l. Whether Plaintiffs and the Class are entitled to actual damages, punitive damages, treble damages, equitable relief, and other relief as a result of Defendant's wrongful conduct.

84. This class action is also appropriate for certification because T-Mobile has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final declaratory and injunctive relief appropriate with respect to the Class in its entirety. T-Mobile's policies and

practices challenged herein apply to and affect Class members uniformly. Plaintiffs' challenge of these policies hinges on T-Mobile's conduct with respect to the Class in its entirety, not on facts or law applicable only to the Plaintiffs.

85. Unless a Class-wide injunction is issued, T-Mobile may continue in its failure to protect and safeguard its customers' sensitive personal and financial information and otherwise act unlawfully as set forth in this Complaint.

CLAIMS FOR RELIEF ON BEHALF OF THE CLASS

FIRST CAUSE OF ACTION
(Declaratory Judgement as to Invalidity of Arbitration Provision and Delegation Clause and Injunctive Relief)

86. Plaintiffs incorporate by reference and reallege paragraphs 1 to 85 contained above, as though fully set forth herein.

87. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in the Complaint.

88. An actual controversy has arisen regarding T-Mobile's duties to its customers and whether T-Mobile is taking adequate measures to protect and safeguard its customers' sensitive personal and financial information. An actual

controversy has also arisen regarding T-Mobile's unconscionable Terms and Conditions.

89. T-Mobile has attempted to immunize itself from liability for its wrongful conduct by burying in a lengthy Terms and Conditions a number of unconscionable provisions, including: a purported arbitration agreement, class action waiver, and jury trial waiver.

90. T-Mobile's purported arbitration agreement, class action waiver, and jury trial wavier are unenforceable because they violate public policy and are both procedurally and substantively unconscionable.

91. Specifically, the arbitration clause in T-Mobile's Terms and Conditions lacks mutuality and imposes an unfair burden on Plaintiffs that qualifies as unconscionable.

92. The Terms and Conditions includes pretextual and unduly onerous preconditions to arbitration.

93. The Terms of Service dispute resolution process is procedurally unconscionable. Moreover, to the extent the Terms of Service expressly or impliedly incorporates a "delegation clause" that "decides who decides" disputes, such delegation clause imposes an onerous, unfair, and unusual burden on users because the delegation clause itself is subject to the multi-step, onerous dispute resolution process in the Terms of Service.

94. T-Mobile's complaint process is ineffective, unavailing, and one-sided; it requires users to jump through antecedent hoops not applicable to T-Mobile before initiating arbitration.

95. A judicial declaration is necessary and appropriate so the parties may ascertain their rights, duties, and obligations with respect to these provisions.

96. The Court may use its equitable powers to declare the arbitration clause, class action waiver, and jury trial waiver in T-Mobile's Terms and Conditions to be unenforceable.

97. Accordingly, Plaintiffs are entitled to a declaration that the arbitration clause, including any delegation clause and dispute resolution notice, class action waiver, and jury trial waiver in the T-Mobile's Terms and Conditions are unconscionable and unenforceable as to Plaintiffs.

SECOND CAUSE OF ACTION
(Federal Communications Act)

98. Plaintiffs incorporate by reference and reallege paragraphs 1 to 85 contained above, as though fully set forth herein.

99. T-Mobile is one of the world's largest telecommunications company and provider of mobile telephone services. As a common carrier,[3] T-Mobile is governed by the Federal Communications Act of 1934, as amended ("FCA"),[4] and

[3] 47 U.S. Code § 153(51).
[4] 47 U.S.C. § 151, *et seq*.

corresponding regulations passed by the FCC.[5] Recognizing the sensitivity of data collected by mobile carriers, Congress, through the FCA, requires T-Mobile to protect Plaintiffs' sensitive personal information to which it has access as a result of its unique position as a telecommunications carrier.[6]

100. Section 222 of the FCA, which became part of the Act in 1996, requires T-Mobile to protect the privacy and security of information about its customers. Likewise, Section 201(b) of the Act requires T-Mobile's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[7] T-Mobile's most specific obligations to protect its customers concerns a specific type of information, called Customer Proprietary Information and Other Customer Information, and known by the acronym "CPNI."[8] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[9]

[5] 47 C.F.R. § 64.2001, *et seq*.
[6] 47 U.S.C. § 222.
[7] 47 U.S.C. § 201(b).
[8] 47 U.S.C. § 222(a).
[9] Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").

101. Carriers like T-Mobile are liable for failures to protect their customers unauthorized disclosures.[10] The FCC has also stated that "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, ... a violation of section 222 may have occurred."[11]

102. CPNI is defined in the FCA as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[12]

103. T-Mobile violated the FCA, 47 U.S.C. § 222(a), by failing to protect the confidentiality of Plaintiffs' CPNI. The FCC has "[made] clear that carriers' existing statutory obligations to protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to

[10] 47 U.S.C. §§ 206, 207.
[11] Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").
[12] 47 U.S.C. § 222(h)(1).

protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[13] The FCA forbids T-Mobile from "us[ing], disclos[ing], or permit[ting] access to" CPNI, except in limited circumstances.[14] This extends to the carrier's employees, representatives, and agents.

104. T-Mobile may only use, disclose, or permit access to Plaintiffs' CPNI: (1) as required by law; (2) with their approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[15] Beyond such use, "the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI."[16]

105. T-Mobile failed to take reasonable steps to protect Plaintiffs' CPNI, but instead turned it over to a hacker without Plaintiffs' authorization. T-Mobile's employees, representatives, and agents, acting within the scope of their employment and agency, likewise did not obtain Plaintiffs' knowing consent before using, disclosing, and/or permitting access to their CPNI when they accessed their accounts and swapped their SIM cards.

106. T-Mobile violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Plaintiffs' CPNI without the notice, consent, and/or legal

[13] 2007 CPNI Order ¶ 36 (citation omitted).
[14] 47 U.S.C. § 222(c)(1).
[15] 47 U.S.C. § 222.
[16] 2007 CPNI Order ¶ 8.

authorization required under the FCA. T-Mobile also caused and/or permitted third parties to use, disclose, and/or permit access to Plaintiffs' CPNI without the notice, consent, and/or legal authorization required under the FCA.

107. Under the FCA, T-Mobile is not just liable for its own violations of the FCA, but also for violations that it "cause[s] or permit[s]."[17] By failing to secure Plaintiffs' accounts and protect their CPNI, T-Mobile caused and/or permitted Plaintiffs' CPNI to be accessed and used by its own employees, representatives and agents and by third-party hackers.

108. T-Mobile is also responsible for the acts, omissions, and/or failures of officers, agents, employees, or any other person acting for or employed by T-Mobile.

109. As a proximate and actual cause of T-Mobile's violations of the FCA, Plaintiffs have suffered injury to their person, property, physical and emotional health (as discussed above), finances, and reputation.

[17] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

110. Plaintiffs seek the full amount of damages sustained as a consequence of T-Mobile's violations of the FCA, as well as reasonable attorneys' fees and costs incurred in prosecuting this action.

THIRD CAUSE OF ACTION
(Negligence)

111. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 85 above as though fully set forth herein.

112. T-Mobile owed a duty to Plaintiffs to exercise reasonable care in safeguarding their sensitive and private personal information. The duty arose from the sensitivity of their T-Mobile account information and the foreseeability of harm to Plaintiffs should Defendant fail to safeguard and protect such data. The duty included, among other things, designing, maintaining, monitoring, and testing T-Mobile's and its agents', partners', and independent contractors' systems, protocols, and practices to ensure that Plaintiffs' information was adequately secured from unauthorized access. Federal law and regulations, as well as T-Mobile's privacy policy, acknowledge T-Mobile's duty to adequately protect Plaintiffs' confidential account information.

113. T-Mobile owed a duty to Plaintiffs to protect their sensitive account data from unauthorized use, access, or disclosure. This included a duty to ensure that their CPNI was used, accessed, or disclosed only with proper consent.

114. T-Mobile had a special relationship with Plaintiffs due to its status as their telecommunications carrier, which provided an independent duty of care. T-Mobile had the unique ability to protect its systems and the data stored thereon from unauthorized access.

115. Plaintiffs' willingness to contract with T-Mobile, and thereby entrust T-Mobile with their confidential and sensitive account data, was predicated on the understanding that T-Mobile and its agents would undertake adequate security and consent precautions.

116. T-Mobile breached its duties by, *inter alia*: (a) failing to implement and maintain adequate security practices to safeguard Plaintiffs' T-Mobile account and data from unauthorized access, as detailed herein; (b) failing to train and supervise its agents and employees and prevent them from accessing and utilizing Plaintiffs' T-Mobile account and data without authorization; (c) reassigning Plaintiffs' phones from the SIM card in the respective Plaintiffs' phone to another SIM card without Plaintiffs' authorization; and (d) failing to provide adequate and timely notice of unauthorized access.

117. But for T-Mobile's breaching the duties it owed to Plaintiffs, Plaintiffs' data would not have been accessed by unauthorized individuals.

118. Plaintiffs were a foreseeable victim of T-Mobile's inadequate data security practices and consent mechanisms. T-Mobile and its agents knew or

should have known that SIM swaps presented a serious threat to its customers, including Plaintiffs. T-Mobile also knew or should have known that improper procedures and systems to safeguard customer data could allow their agents and employees to authorize customers' accounts and data.

119. T-Mobile knew or should have known that unauthorized access would cause damage to Plaintiffs. T-Mobile has publicly acknowledged that unauthorized account access presents a significant threat to its customers.

120. T-Mobile's negligent conduct provided a means for unauthorized individuals to access Plaintiffs' account data, to take over control of their respective mobile phones, and use such access to hack into numerous online accounts in order to steal Plaintiffs' assets and personal information. As a result of T-Mobile's failure to prevent unauthorized access, Plaintiffs suffered grave injury, as alleged fully above, including severe physical and emotional distress. Plaintiffs' injuries arose directly out of T-Mobile's breach of its legal duties. The damages Plaintiffs suffered were a proximate, reasonably foreseeable result of T-Mobile's breaches of their duties. Therefore, Plaintiffs are entitled to damages in an amount to be proven at trial.

121. The injury and harm suffered by Plaintiffs was the reasonably foreseeable result of T-Mobile's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' Personal Information, including their CPI and CPNI.

122. As a direct and proximate result of T-Mobile's negligence, Plaintiffs suffered great personal and financial harm by the intrusion into their private affairs, loss of money and other assets, and compromise of their personally identifiable information, as detailed throughout this Complaint.

123. T-Mobile's negligence was a substantial factor in causing the harm suffered by Plaintiff. But for T-Mobile's negligence, the unauthorized third parties would not have been a victim of SIM swap theft resulting in the loss of millions of dollars and the breach of sensitive personal information.

124. Furthermore, had it not been for T-Mobile's negligence, Plaintiffs would not have sustained the physical, emotional, and financial damages described herein.

FOURTH CAUSE OF ACTION
(Negligent Hiring, Retention, and Supervision)

125. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 85 above as though fully set forth herein.

126. At all material times herein, T-Mobile's agents, officers, and employees, including, but not limited to, those directly or indirectly responsible for or involved in allowing unauthorized access to Plaintiffs' confidential and proprietary account information, were under T-Mobile's direct supervision and control.

127. Upon information and belief, T-Mobile negligently hired, retained, controlled, trained, and supervised the officers, agents, and employees under its control, or knew or should have known that such officers, agents, and employees were negligently hired, retained, controlled, trained, and supervised with regard to unauthorized access to customer accounts.

128. Upon information and belief, T-Mobile negligently failed to implement systems and procedures necessary to prevent its officers, agents, and employees from allowing or obtaining unauthorized access to customer accounts, including that of Plaintiffs.

129. Upon information and belief, T-Mobile's negligent hiring, retention, control, training, and supervision allowed the unauthorized access to customers' accounts resulting in damage to T-Mobile customers and foreseeable victims in the public at large, including Plaintiffs.

130. Given T-Mobile's experience with account takeover and SIM-swap attacks (including some perpetrated and/or assisted by T-Mobile's own employees, officers or agents), T-Mobile's failure to exercise reasonable care in hiring, retaining, controlling, training, and supervising its officers, agents and employees was a breach of its duty to its customers, including Plaintiffs.

131. T-Mobile's duty to its customers and foreseeable victims to protect its customers' data from unauthorized access is required by federal and state law.

132. It was entirely foreseeable to T-Mobile that unauthorized persons would attempt to gain unauthorized access to T-Mobile customers' data and, despite this, T-Mobile failed to implement sufficient safeguards and procedures to prevent its officers, agents and employees from granting or obtaining such unauthorized access.

133. Upon information and belief, T-Mobile engaged in the acts alleged herein and/or condoned, permitted, authorized and/or ratified the conduct of its officers, agents and employees.

134. As a direct consequence of T-Mobile's negligent hiring, retention, controlling, training, and supervision of its officers, agents and employees, who enabled or obtained the unauthorized access to Plaintiffs' accounts, Plaintiffs were damaged through the loss of millions of dollars and the breach of sensitive personal information.

FIFTH CAUSE OF ACTION
(Breach of Contract and the Implied Covenant of Good Faith and Fair Dealing)

135. Plaintiffs incorporate by reference and realleges paragraphs 1 to 85 contained above, as though fully set forth herein.

136. Plaintiffs have purportedly entered into a written contract, the Terms and Conditions which includes the incorporated Rate Plan, with T-Mobile. Plaintiffs were presented with the Terms and Conditions on a take-it-or-leave it

basis and had no opportunity to negotiate any of the specific terms or provisions thereunder.

137. Every contract, including the Terms and Conditions, contains an implied duty of good faith and fair dealing. T-Mobile entered into and are bound by the Terms and Conditions with Plaintiffs, which are valid and enforceable contracts that contain an implied duty of good faith and fair dealing.

138. T-Mobile breached the Terms and Conditions and the implied covenant of good faith and fair dealing by, among other things, failing to discharge their obligations and provide the services they promised in exchange for the fees they charged Plaintiffs.

139. T-Mobile breached the Terms and Conditions and the implied covenant of good faith and fair dealing by failing to protect and safeguard its customers' sensitive personal and financial information.

140. As a result of T-Mobile's breach of its contractual duties, obligations and/or promises arising under the Terms and Conditions and the implied covenant of good faith and fair dealing, Plaintiffs were damaged by, including but not limited to, the loss of millions of dollars in cryptocurrency and the breach of sensitive personal information, all in an amount to be proven at trial.

141. In addition to Plaintiffs' actual contract damages, Plaintiffs seek recovery of their attorney's fees, costs to the extent provided by the Terms and Conditions and pre-judgment interest.

SIXTH CAUSE OF ACTION
(Computer Fraud and Abuse Act)

142. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 85 above as though fully set forth herein.

143. Plaintiffs' mobile devices are capable of connecting to the Internet.

144. The CFAA governs those who intentionally access computers without authorization or who intentionally exceed authorized access and as a result of such conduct, cause damage and loss.

145. Section 1030(g) of the CFAA provides, in pertinent part:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brough under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage….

146. T-Mobile's agents and employees, in the scope of their employment, intentionally accessed Plaintiffs' mobile devices, and assisted others in accessing Plaintiffs' mobile devices, without Plaintiffs' authorization.

147. T-Mobile is liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, agents, or any other person acting for on behalf of T-Mobile.

148. T-Mobile violated the CFAA by exceeding its authority to access the computer data and breach the confidentiality of the proprietary information of Plaintiffs using, disclosing, or permitting access to Plaintiffs' CPNI without the consent, notice, and/or legal authorization of Plaintiffs as required by the CFAA.

149. As a result of T-Mobile's actions, Plaintiffs suffered damage to information on their mobile devices, including being unable to access information and data on their mobile devices and being unable to access personal email, cryptocurrency, and other sensitive accounts.

150. Plaintiffs have brought this claim within two (2) years of the date of discovery of the damage pursuant to Section 1030(g) of the CFAA.

151. As a direct and proximate result of T-Mobile's illegal acts, Plaintiffs suffered great personal and financial harm, as detailed throughout this Complaint. The financial harm suffered by Plaintiffs exceeds $5,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against T-Mobile as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class as requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order for declaratory and injunctive relief, including public injunctive relief, and for money damages under Federal Rules of Civil Procedure Rule 23, appointing Plaintiffs as Class Representatives, and appointing their attorneys as Class Counsel;

d. An order for declaratory relief that the arbitration clause, including any delegation clause and dispute resolution notice, class action waiver, and jury trial waiver in the T-Mobile's Terms and Conditions are unconscionable and unenforceable as to Plaintiffs and the Class;

e. A judgment for actual damages;

f. A judgment for compensatory damages;

g. A judgment for injunctive relief enjoining T-Mobile from engaging in future unlawful activities complained of herein, including violations of the federal and state laws raised in the Complaint;

h. An order directing T-Mobile to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and regulations and to protect T-Mobile customers from a repeat of the damaging events described herein, including, but not limited to, putting forward for stockholder vote, resolutions for amendments to the Company's Bylaws or Articles of Incorporation and taking such other action as may be necessary to place before stockholders for a vote of the following corporate governance policies:

i. a proposal to enhance security and cybersecurity around data privacy and system security;
ii. a proposal to strengthen Board oversight and supervision of T-Mobile's security and cybersecurity practices;
iii. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater stockholder input into the policies and guidelines of the Board;
iv. a proposal to appoint at least two additional independent board members with established reputations in cybersecurity and with substantial experience in governance, risk, compliance and particularly cybersecurity issues;
v. a proposal to enhance and/or augment the audit, risk and compliance committees of the Board to oversee internal controls and compliance processes;
vi. a proposal to ensure that the Chief Information Security Officer (CISO); Chief Compliance (CCO); Chief Risk

Officer (CRO); Chief Legal Officer(s) (CLO); and other company leadership have (1) necessary subject matter and regulatory expertise; (2) direct reporting authority to the Board; and (3) adequate autonomy and resources to carry out their responsibilities;

vii. a proposal to review and implement revised codes of conduct, policies and procedures, training, integrity hotlines, auditing and monitoring processes and procedures;

viii. a proposal to review and implement policies and procedures for escalating internal cybersecurity and regulatory issues internally and to the Board; and

ix. a proposal to review and implement the confidential reporting structure and investigative process of complaints within the company.

i. A judgment for exemplary and punitive damages for Defendant's knowing, willful, and/or intentional conduct;

j. Pre-judgment and post-judgment interest;

k. A judgment for reasonable attorney fees and costs of this suit, pursuant to O.C.G.A. § 13-6-11 due to T-Mobile's bad faith and stubborn litigiousness, O.C.G.A. § 10-1-393, and other applicable statutes;

l. A judgment for all such other and further relief as the Court deems equitable, up to an including appointment or a corporate monitor to oversee cybersecurity enhancements.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: December 21, 2022

HERMAN JONES LLP

By: */s/ Gregory F. Wesner*

Gregory F. Wesner, WSBA No. 30241
HERMAN JONES LLP
15113 Washington Ave NE
Bainbridge Island, WA 98110
Tel.: (206) 819-0821
gwesner@hermanjones.com

John C. Herman
Peter M. Jones
Serina M. Vash
(to seek admission *pro hac vice*)
3424 Peachtree Road, N.E., Suite 1650
Atlanta, Georgia 30326
Telephone: (404) 504-6500
Facsimile: (404) 504-6501
jherman@hermanjones.com
pjones@hermanjones.com
svash@hermanjones.com

Counsel for Plaintiffs